Věta o dělení polynomů se zbytkem

Věta. *Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.*

Důkaz existence q, r. Pro $f = 0$ zřejmé ($q = r = 0$), dále $f \neq 0$.
Nechť $g = a_n x^n + \cdots + a_1 x + a_0$, $a_n \in R^\times$, tj. $\mathrm{st}(g) = n$,
$f = b_m x^m + \cdots + b_1 x + b_0$, $b_m \neq 0$, tj. $\mathrm{st}(f) = m$.
Postupujme indukcí vůči m.
I. krok: Je-li $m < n$, pak označme $q = 0$, $r = f$.
II. krok: Předpokládejme, že $m \geq n$ a že pro polynomy stupně menšího než m již bylo dokázáno. Polynom $g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n}$ má stejný stupeň i vedoucí koeficient jako f, proto pro polynom $h = f - g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n}$ platí $\mathrm{st}(h) < m$. Z indukčního předpokladu existují $p, r \in R[x]$ tak, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $h = g \cdot p + r$. Pak dosazením a úpravou dostaneme
$f = g \cdot a_n^{-1} \cdot b_m \cdot x^{m-n} + h = g \cdot (a_n^{-1} \cdot b_m \cdot x^{m-n} + p) + r$.
Stačí označit $q = a_n^{-1} \cdot b_m \cdot x^{m-n} + p$.

Věta o dělení polynomů se zbytkem

Věta. Nechť R je okruh, $f, g \in R[x]$, přičemž vedoucí koeficient polynomu $g \neq 0$ je jednotka okruhu R. Pak existuje jediná dvojice polynomů $q, r \in R[x]$ taková, že $\mathrm{st}(r) < \mathrm{st}(g)$ a platí $f = g \cdot q + r$.

Důkaz jednoznačnosti q, r. Předpokládejme, že $q, r, \bar{q}, \bar{r} \in R[x]$, přičemž $\mathrm{st}(r) < \mathrm{st}(g)$ a $\mathrm{st}(\bar{r}) < \mathrm{st}(g)$, splňují $f = g \cdot \bar{q} + \bar{r} = g \cdot q + r$. Pak $g \cdot (\bar{q} - q) = r - \bar{r}$. Vedoucí koeficient polynomu g není dělitel nuly, tedy $\mathrm{st}(g) + \mathrm{st}(\bar{q} - q) = \mathrm{st}(g \cdot (\bar{q} - q)) = \mathrm{st}(r - \bar{r}) < \mathrm{st}(g)$. Pak tedy $\mathrm{st}(\bar{q} - q) < 0$, tj. $\bar{q} = q$, odkud $\bar{r} = r$.

Euklidův algoritmus v okruhu polynomů nad tělesem

Poznámka. Je-li R je těleso, je v $R[x]$ vedoucí koeficient každého nenulového polynomu jednotkou. Proto pro libovolné nenulové polynomy $f, g \in R[x]$ lze postupovat podle Euklidova algoritmu

$$\begin{aligned} f &= g \cdot q_0 + r_0, \\ g &= r_0 \cdot q_1 + r_1, \\ r_0 &= r_1 \cdot q_2 + r_2, \\ r_1 &= r_2 \cdot q_3 + r_3, \\ &\vdots \\ r_{n-2} &= r_{n-1} \cdot q_n + r_n, \\ r_{n-1} &= r_n \cdot q_{n+1} + 0. \end{aligned}$$

Přitom $\mathrm{st}(g) > \mathrm{st}(r_0) > \mathrm{st}(r_1) > \mathrm{st}(r_2) > \ldots$, proto skutečně po několika děleních nastane $r_{n+1} = 0$.

Největší společný dělitel v okruhu polynomů nad tělesem

Věta. *Nechť R je těleso. Pak libovolné dva nenulové polynomy $f, g \in R[x]$ mají v $R[x]$ největší společný dělitel $d \in R[x]$, který je možné spočítat pomocí Euklidova algoritmu (jako poslední nenulový zbytek v prováděných děleních) a vyjádřit jej Bezoutovou rovností, tj. existují $a, b \in R[x]$ tak, že $d = a \cdot f + b \cdot g$.*

Definice. Nenulový polynom se nazývá **normovaný**, je-li jeho vedoucí koeficient roven 1.

Poznámka. Jeli R těleso, je $R[x]$ obor integrity a platí $(R[x])^\times = R^\times = R^*$. Je tedy každý nenulový polynom z $R[x]$ asociovaný s právě jedním normovaným.

Definice. Nechť R je těleso, $f, g \in R[x]$ nenulové polynomy. Označme (f, g) normovaný největší společný dělitel polynomů f a g. O polynomech f a g řekneme, že jsou **nesoudělné**, je-li $(f, g) = 1$.

Věta. *Nechť R je těleso, $f, g, h \in R[x]$ nenulové polynomy. Jestliže $f \mid g \cdot h$ a současně $(f, g) = 1$, pak $f \mid h$.* Důkaz.

Ireducibilní polynomy

Věta. *Nechť R je těleso, $f \in R[x]$. Polynom f je ireducibilní prvek okruhu $R[x]$, právě když f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.*

Definice. Nechť R je okruh, $f \in R[x]$ se nazývá **ireducibilní polynom nad** R, jestliže f není konstantní a nelze jej rozložit na součin dvou nekonstantních polynomů z okruhu $R[x]$.

Varování. Pozor, rozlišujte pojmy „ireducibilní polynom nad okruhem R“ a „ireducibilní prvek okruhu $R[x]$.“

Příklad. Je-li R těleso, jsou ireducibilní polynomy nad R právě ireducibilními prvky okruhu $R[x]$.

Příklad. Konstantní polynom 2 je ireducibilním prvkem okruhu $\mathbb{Z}[x]$, ale není ireducibilním polynomem nad $\mathbb{Z}$. Polynom $2x$ je ireducibilní polynom nad $\mathbb{Z}$, ale není ireducibilním prvkem okruhu $\mathbb{Z}[x]$.

Věta. *Nechť R je těleso, $f, g, h \in R[x]$ polynomy, přičemž f je ireducibilní nad R. Jestliže $f \mid g \cdot h$, pak $f \mid g$ nebo $f \mid h$.*

Okruh polynomů nad libovolným tělesem je okruhem s jednoznačným rozkladem

Věta. *Nechť R je těleso, $f \in R[x]$ nenulový polynom. Pak existuje $k \in \mathbb{Z}$, $k \geq 0$, $a \in R^*$ a normované ireducibilní polynomy $p_1, \ldots, p_k \in R[x]$ tak, že*

$$f = a \cdot p_1 \cdot \ \ldots \ \cdot p_k.$$

Tento rozklad je navíc jednoznačný až na pořadí činitelů.

Důsledek. *Jestliže R je těleso, je $R[x]$ okruh s jednoznačným rozkladem.*

Poznámka. Předchozí důsledek lze značně zesílit, platí totiž následující věta:

Věta. *Nechť R je okruh. Pak okruh polynomů $R[x]$ je okruhem s jednoznačným rozkladem, právě když okruh R je okruhem s jednoznačným rozkladem.*

Důsledek. *Okruh $\mathbb{Z}[x]$ je okruhem s jednoznačným rozkladem.*

Kořen polynomu

Definice. Nechť R je okruh, $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$, $c \in R$. Pak prvek $a_n \cdot c^n + \cdots + a_1 \cdot c + a_0 \in R$ značíme $f(c)$ a nazýváme **hodnota** polynomu f v prvku c.

Věta. Nechť R je komutativní okruh, $f, g \in R[x]$, $c \in R$. Pak platí

- $(f + g)(c) = f(c) + g(c)$,
- $(f \cdot g)(c) = f(c) \cdot g(c)$.

Poznámka. Předpoklad o komutativitě byl podstatný pro násobení: jestliže pro $a, c \in R$ platí $a \cdot c \neq c \cdot a$, pak pro $f = x$, $g = a$ je $(f \cdot g)(c) = (x \cdot a)(c) = (ax)(c) = a \cdot c \neq c \cdot a = f(c) \cdot g(c)$.

Důsledek. Nechť R je komutativní okruh, $c \in R$. Pak zobrazení $\alpha : R[x] \to R$ určené předpisem $\alpha(f) = f(c)$ pro každé $f \in R[x]$ je homomorfismus okruhů.

Definice. Nechť R je okruh, $f \in R[x]$, $c \in R$. Řekneme, že c je **kořenem** polynomu f, jestliže $f(c) = 0$.

Násobnost kořene polynomu

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$. Pak platí: c je kořenem polynomu f, právě když $(x-c) \mid f$ v okruhu $R[x]$.* Důkaz.

Definice. Nechť R je komutativní okruh, $f \in R[x]$, $f \neq 0$, $c \in R$, $f(c) = 0$. Přirozené číslo k se nazývá **násobnost** kořene c polynomu f, jestliže $(x-c)^k \mid f$ a $(x-c)^{k+1} \nmid f$ v okruhu $R[x]$. Kořeny násobnosti 1 se nazývají **jednoduché**.

Poznámka. Podmínka $(x-c)^k \mid f$ znamená, že existuje $g \in R[x]$ tak, že $(x-c)^k \cdot g = f$. Protože $(x-c)^k$ je normovaný polynom stupně k, platí $k + \mathrm{st}(g) = \mathrm{st}(f)$. Přitom $g \neq 0$, tedy $\mathrm{st}(g) \geq 0$, odkud plyne $k \leq \mathrm{st}(f)$. Proto nenulový polynom nemůže být dělitelný každou mocninou polynomu $x-c$ a předchozí definice jednoznačně určuje násobnost každého kořene libovolného nenulového polynomu nad komutativním okruhem.

Příklad. Kvadratický polynom $x^2 - [1]_8 \in \mathbb{Z}_8[x]$ má čtyři jednoduché kořeny $[1]_8$, $[-1]_8$, $[3]_8$, $[-3]_8$. V okruhu $\mathbb{Z}_8[x]$ není rozkládání na součin normovaných lineárních činitelů jednoznačné.

Počet kořenů polynomu nad oborem integrity

Věta. *Nechť R je obor integrity, $f \in R[x]$, $f \neq 0$. Polynom f má nejvýše* $\mathrm{st}(f)$ *kořenů v R, počítáno i s násobností. Přesněji: součet násobností všech kořenů polynomu f v R je menší nebo roven* $\mathrm{st}(f)$.

Důkaz. Nechť $c_1, \ldots, c_s$ jsou různé kořeny polynomu f v R, nechť k_i je násobnost kořene c_i. Pak $(x - c_i)^{k_i} \mid f$ v $R[x]$. Označme K podílové těleso oboru integrity R, tedy R je podokruhem tělesa K. Pak $(x - c_i)^{k_i} \mid f$ v $K[x]$. Přitom $x - c_1, \ldots, x - c_s$ jsou různé normované ireducibilní polynomy v $K[x]$. Rozložíme-li f na součin vedoucího koeficientu f a normovaných ireducibilních polynomů v $K[x]$, z jednoznačnosti rozkladu plyne, že se mezi nimi polynom $x - c_i$ objeví alespoň k_i-krát pro každé $i = 1, \ldots, s$. Proto $\prod_{i=1}^{s} (x - c_i)^{k_i} \mid f$. Protože K je těleso, platí $\sum_{i=1}^{s} k_i \leq \mathrm{st}(f)$.

Důsledek. *Nechť R je konečné těleso, pak je jeho multiplikativní grupa $(R^*, \cdot)$ cyklická.* Důkaz.

Důsledek. *Pro libovolné prvočíslo p je grupa $(\mathbb{Z}_p^\times, \cdot)$ cyklická.*

Derivace polynomu

Definice. Nechť R je okruh, $f = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$ polynom z $R[x]$. **Derivací** polynomu f rozumíme polynom

$$f' = n a_n x^{n-1} + \cdots + 2 a_2 x + a_1.$$

Poznámka. V tělese reálných čísel máme pojem limity, který v obecném okruhu není k dispozici. Proto jsme pojem derivace polynomu nemohli definovat limitou, ale jen uvedeným vzorcem, v němž například $n a_n$ znamená n-násobek prvku a_n (tedy součet n kopií prvku a_n v grupě $(R, +)$).

Věta. Nechť R je okruh, $f, g \in R[x]$, $c \in R$. Pak platí

- $(f + g)' = f' + g'$,
- $(f \cdot g)' = f' \cdot g + f \cdot g'$,
- $((x - c)^n)' = n(x - c)^{n-1}$.

Označení. Druhou derivaci polynomu f značíme $f'' = (f')'$, třetí $f''' = (f'')'$ atd. Obecně pro $k \in \mathbb{N}$ pak k-tou derivaci polynomu f značíme $f^{(k)} = (f^{(k-1)})'$. Je tedy $f^{(1)} = f'$, $f^{(2)} = f''$, atd.

Souvislost derivace polynomu s násobností kořenů

Věta. *Nechť R je komutativní okruh, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Jestliže c je k-násobným kořenem polynomu f, pak je c kořenem polynomů f', f'', $\ldots$, $f^{(k-1)}$.* Důkaz.

Věta. *Nechť R je těleso, $f \in R[x]$, $c \in R$, $k \in \mathbb{N}$. Předpokládejme, že* $\operatorname{char} R = 0$ *nebo* $\operatorname{char} R > k$. *Pak c je k-násobným kořenem polynomu f, právě když je c kořenem polynomů f', f'', $\ldots$, $f^{(k-1)}$ a není kořenem polynomu $f^{(k)}$.*

Příklad. Předpoklad o charakteristice je nezbytný. Například pro $R = \mathbb{Z}_2$ polynom $f = x^2 \in \mathbb{Z}_2[x]$ má kořen $[0]_2$ násobnosti 2. Přitom $f' = 2[1]_2 x = 0$, a tedy $f^{(k)} = 0$ pro každé $k \in \mathbb{N}$.

Poznámka. Jev pozorovaný v předchozím příkladě platí obecněji: je-li $\operatorname{char} R = p > 0$, pak pro každé $f \in R[x]$ platí $f^{(p)} = 0$.

Polynomy nad $\mathbb{C}$

Věta (Základní věta algebry). *Každý nekonstantní polynom $f \in \mathbb{C}[x]$ má v $\mathbb{C}$ kořen.*

Definice. Těleso R se nazývá **algebraicky uzavřené**, jestliže každý nekonstantní polynom $f \in R[x]$ má v R kořen.

Příklad. Tělesa $\mathbb{R}$ a $\mathbb{Q}$ nejsou algebraicky uzavřená, žádné konečné těleso není algebraicky uzavřené (je-li $R = \{r_1, \ldots, r_n\}$, pak $(x - r_1) \cdot \ \ldots \ \cdot (x - r_n) + 1$ nemá v R kořen).

Poznámka. Základní větu algebry lze tedy formulovat takto: *$\mathbb{C}$ je algebraicky uzavřené těleso.*

Důsledek. *Pro libovolný polynom $f \in \mathbb{C}[x]$ platí: f je ireducibilní nad $\mathbb{C}$, právě když je f lineární.*

Důsledek. *Nechť $f \in \mathbb{C}[x]$ je normovaný polynom, $\mathrm{st}(f) = n \geq 1$. Pak existují $c_1, \ldots, c_n \in \mathbb{C}$ tak, že*

$$f = (x - c_1) \cdot \ \ldots \ \cdot (x - c_n).$$

Tento rozklad je navíc jednoznačný až na pořadí činitelů.

Polynomy nad $\mathbb{C}$ - Viètovy vztahy

Důsledek (Viète). Nechť $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ *je normovaný polynom,* $n \geq 1$, $c_1, \ldots, c_n \in \mathbb{C}$ *jeho kořeny (každý uveden tolikrát, kolik je jeho násobnost). Pak platí*

$$\begin{aligned}
-a_{n-1} &= c_1 + \cdots + c_n, \\
a_{n-2} &= c_1c_2 + c_1c_3 + \cdots + c_1c_n + c_2c_3 + \cdots + c_{n-1}c_n, \\
&\vdots \\
(-1)^k a_{n-k} &= \sum_{1 \leq i_1 < \cdots < i_k \leq n} c_{i_1} c_{i_2} \ldots c_{i_k}, \\
&\vdots \\
(-1)^n a_0 &= c_1 c_2 \ldots c_n.
\end{aligned}$$

Poznámka. Výraz na pravé straně k-tého řádku lze popsat takto: vezmeme všechny k-prvkové podmnožiny množiny indexů $\{1, 2, \ldots, n\}$, pro každou z nich vynásobíme odpovídající kořeny a získané součiny sečteme.

Polynomy nad $\mathbb{R}$

Věta. *Je-li komplexní číslo c kořenem polynomu $f \in \mathbb{R}[x]$, pak i číslo $\overline{c}$ komplexně sdružené s číslem c je kořenem polynomu f.*

Věta. *Pro libovolný polynom $f \in \mathbb{R}[x]$ platí: f je ireducibilní nad $\mathbb{R}$, právě když je f lineární anebo je $f = ax^2 + bx + c$ kvadratický se záporným diskriminantem $b^2 - 4ac < 0$.* Část důkazu.

Důsledek. *Každý nekonstantní normovaný polynom $f \in \mathbb{R}[x]$ lze psát jako součin normovaných polynomů, které jsou lineární anebo kvadratické se záporným diskriminantem. Tento zápis je jednoznačný až na pořadí činitelů.*

Polynomy nad $\mathbb{Z}$ - hledání racionálních kořenů

Věta. *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n, $r \in \mathbb{Z}$, $s \in \mathbb{N}$, $(r, s) = 1$, *taková, že* $\frac{r}{s}$ *je kořen polynomu. Pak platí*

- $r \mid a_0$,
- $s \mid a_n$,
- *pro každé* $m \in \mathbb{Z}$ *platí* $(sm - r) \mid f(m)$.

Poznámka. Předchozí větu používáme pro nalezení všech racionálních kořenů daného polynomu s celočíselnými koeficienty a nenulovým absolutním členem: první dvě podmínky totiž dávají jen konečně mnoho možných hodnot pro r, s. Pro každou z možných dvojic r, s lze zjistit dosazením, zda $\frac{r}{s}$ je kořenem f. V případě velkého počtu dvojic je možné některé dvojice eliminovat třetí podmínkou, například testovat, zda platí $(s + r) \mid f(-1)$ a $(s - r) \mid f(1)$.

Polynomy nad $\mathbb{Z}$

Definice. Nechť $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ je nenulový. Řekneme, že f je **primitivní**, jestliže jeho koeficienty jsou nesoudělné, tj. $(a_0, a_1, \ldots, a_n) = 1$.

Věta (Gaussovo lemma). Součin libovolných dvou primitivních polynomů je primitivní polynom.

Důkaz sporem. Přepokládejme, že $f, g \in \mathbb{Z}[x]$ jsou primitivní polynomy takové, že jejich součin $f \cdot g$ primitivní není. Pak existuje prvočíslo p, které dělí všechny koeficienty polynomu $f \cdot g$.
Zobrazení $\alpha : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ určené předpisem

$$\alpha(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) = \\ = [a_n]_p x^n + [a_{n-1}]_p x^{n-1} + \cdots + [a_1]_p x + [a_0]_p$$

pro libovolné $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ (tedy každý koeficient je nahrazen odpovídající zbytkovou třídou) je homomorfismus okruhů. Pak $\alpha(f) \neq 0$, $\alpha(g) \neq 0$, $\alpha(f) \cdot \alpha(g) = \alpha(f \cdot g) = 0$, což je spor s tím, že $\mathbb{Z}_p$ je těleso, a tedy $\mathbb{Z}_p[x]$ je obor integrity.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Gauss). Libovolný polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

Důkaz. Tvrzení je zřejmé pro konstantní polynom f, který není ireducibilní ani nad $\mathbb{Z}$ ani nad $\mathbb{Q}$. Nechť je tedy f nekonstantní. Jestliže f není ireducibilní nad $\mathbb{Z}$, je možné jej psát jako součin dvou nekonstantníchch polynomů v $\mathbb{Z}[x]$. Tyto polynomy jsou i z $\mathbb{Q}[x]$, a tedy f není ireducibilní nad $\mathbb{Q}$.
Předpokládejme tedy naopak, že f není ireducibilní nad $\mathbb{Q}$. Pak tedy $f = g \cdot h$ pro vhodné nekonstantní polynomy $f, g \in \mathbb{Q}[x]$. Existují nenulová racionální čísla b, c tak, že $b \cdot g$ a $c \cdot h$ jsou primitivní. Podle Gaussova lemmatu je i $(b \cdot g)(c \cdot h) = (bc) \cdot f$ primitivní. Existují nesoudělná $u, v \in \mathbb{N}$ tak, že $bc = \pm\frac{u}{v}$. Kdyby $u \neq 1$, bylo by u dělitelné nějakým prvočíslem p, které by pak dělilo všechny koeficienty polynomu uf a z $p \nmid v$ bychom dostali, že $(bc) \cdot f$ není primitivní. Proto $u = 1$ a $f = (\pm v \cdot (b \cdot g)) \cdot (c \cdot h)$ je rozklad f na součin dvou nekonstantních polynomů v $\mathbb{Z}[x]$, a tedy f není ireducibilní nad $\mathbb{Z}$.

Polynomy nad $\mathbb{Z}$ - ireducibilita

Věta (Eisensteinovo kriterium). *Nechť* $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *je nekonstantní polynom stupně* n. *Jestliže existuje prvočíslo* p *takové, že*

- $p \mid a_{n-1}$, $p \mid a_{n-2}$, $\ldots$, $p \mid a_1$, $p \mid a_0$,
- $p \nmid a_n$,
- $p^2 \nmid a_0$,

pak je f *ireducibilní nad* $\mathbb{Q}$.

Poznámka. Pokud prvočíslo daných vlastností neexistuje, neříká Eisensteinovo kriterium o ireducibilitě f zhola nic.

Polynomy nad $\mathbb{Z}$ - důkaz Eisensteinova kriteria

Důkaz sporem. Předpokládejme, že naopak f není ireducibilní nad $\mathbb{Q}$, podle Gaussovy věty není ireducibilní ani nad $\mathbb{Z}$. Z předpokladů $\mathrm{st}(f) = n > 0$ a f je nekonstantní. Existují tedy nekonstantní polynomy $g, h \in \mathbb{Z}[x]$ tak, že $f = g \cdot h$. Opět užijme homomorfismus okruhů $\alpha : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ určený předpisem

$$\alpha(b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0) = \\ = [b_n]_p x^n + [b_{n-1}]_p x^{n-1} + \cdots + [b_1]_p x + [b_0]_p$$

pro libovolné $b_0, b_1, \ldots, b_n \in \mathbb{Z}$. Pak z prvního předpokladu plyne, že

$$\alpha(g) \cdot \alpha(h) = \alpha(g \cdot h) = \alpha(f) = [a_n]_p x^n$$

je asociované s polynomem x^n, neboť $p \nmid a_n$. Přitom $\mathbb{Z}_p[x]$ je okruh s jednoznačným rozkladem, proto $\alpha(g)$ i $\alpha(h)$ jsou asociované s mocninami polynomu x. A protože jsou nekonstantní, musí být absolutní členy obou polynomů g i h dělitelné p. Jejich součin a_0 je tedy dělitelný p^2, což je spor.